UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/813,003	03/31/2004	Jerry Chow	NRT.0199US (15392ROUS04U)	5213

21906 7590 05/20/2008

TROP PRUNER & HU, PC
1616 S. VOSS ROAD, SUITE 750
HOUSTON, TX 77057-2631

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
05/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/813,003	CHOW, JERRY	
	Examiner	Art Unit	
	JUNG KIM	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20,22-30,32,34-36,39 and 41-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20,22-30,32,34-36,39 and 41-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response to the amendment filed on 2/8/08.

2. Claims 1-20, 22-30, 32, 34-36, 39, 41-45 are pending.

Response to Arguments

3. Applicant's arguments with respect to the amended claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

4. Claims 22-25, 30, 32, 34 and 35 are rejected under 35 U.S.C. 102(b) as being anticipated by Bryant et al. US 5,628,023 (hereinafter Bryant).

5. As per claims 22-25, 30, 32 and 34, Bryant discloses a method of protecting memory in an electronic device, comprising:

a. receiving a memory command to alter a protected memory location; determining whether the received memory command is a memory read command to read the protected memory location, or a memory write command to alter the protected memory location (col. 21:3-21; fig. 3); in response to determining that the received memory command is the memory write command:

i. identifying a memory protection key corresponding to the protected memory location; determining whether the memory command includes the

memory protection key corresponding to the protected memory location; permitting completion of the memory command where the memory command includes the memory protection key corresponding to the protected memory location (fig. 3, reference nos. 540, 560); and rendering the memory protection key in the memory command inaccessible (by virtue of de-allocating memory; see also applicant's specification, pg. 17, lines 19-26); and

b. in response to determining that the received memory command is the memory read command, processing the memory read command to read the protected memory location without checking for any memory protection key; (21:15-18)

c. wherein permitting comprises performing the memory write command (fig. 3, reference no. 570);

d. wherein receiving comprises receiving the memory command from an originating electronic device component, and wherein permitting comprises allowing the originating electronic device component to perform the memory write command; (fig. 1, reference nos. 100, 105, 110)

e. receiving data to be written to the protected memory location; and generating the memory write command responsive to receiving the data (fig. 3, reference no. 540);

f. wherein identifying comprises identifying a protected memory location in the memory write command and accessing a mapping table that maps protected

memory locations to respective corresponding memory protection keys (fig. 1, reference nos. 140, 145, 155, 175 and 185);

g. further comprising: receiving memory commands to alter unprotected memory locations; and permitting completion of the memory commands to alter unprotected memory locations without checking for any memory protection keys (unprotected memory does not require verification);

h. wherein the identifying step comprises accessing the memory protection key corresponding to the protected memory location in a key store, the method further comprising:

ii. receiving a command to establish a new protected memory location in the memory and a memory protection key corresponding to the new protected memory location; establishing the new protected memory location in the memory; and storing the memory protection key in the key store. (fig. 3, reference nos. 485-530; figs. 7 and 9)

6. As per claim 35, Bryant further discloses a computer-readable medium storing instructions for performing the method of claim 22. (fig. 1)

Claim Rejections - 35 USC § 103

7. Claims 1, 2, 4, 7-9 and 11-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beukema et al. US Patent Application Publication No. 20020124148 (hereinafter Beukema) in view of Starek et al. US 5,991,778 (hereinafter Starek)

8. As per claims 1, 2, 4, 7-9 and 11-15, Beukema discloses a memory protection system comprising:

i. a key store storing identifiers of protected memory locations and respective corresponding memory protection keys; and a memory access manager configured to receive a memory command for altering contents of any of the protected memory locations, determine whether the memory command includes a memory protection key corresponding to at least one of said protected memory locations to be altered, if the memory command includes the memory protection key corresponding to each protected memory location to be altered, permit the memory command to proceed, and then render the memory protection key in the memory command inaccessible (paragraph 54; by virtue of de-allocating memory; see also applicant's specification, pg. 17, lines 19-26);

j. wherein the identifiers comprise addresses in a protected memory; wherein the identifiers identify data entries in a protected memory; (paragraph 54; pointer to an associated memory region/address)

k. wherein the key store stores a mapping table that maps each identifier to a corresponding memory protection key; (paragraph 54; "Protection/Translation Table");

l. wherein at least one of the identifiers is mapped to multiple corresponding memory protection keys (paragraph 54; L_key and R_key);

m. the system implemented in an electronic device having a memory, the memory comprising the protected memory locations and unprotected memory locations (paragraph 55, and fig. 6);

n. wherein the memory access manager is further configured to perform the memory command that includes the memory protection key corresponding to each protected memory location to be altered (paragraphs 54 and 59);

o. the system implemented in an electronic device, wherein the memory command is received by the memory access manager from an originating electronic device component, and wherein the originating electronic device component proceeds with the memory command permitted by the memory access manager; wherein the originating electronic device component is a memory update module; wherein the originating electronic device component sends memory commands to the memory access manager responsive to data received at the electronic device; wherein the originating electronic device component is further configured to extract a received memory protection key from the received data and to provide the received memory protection key to the memory access manager. (fig. 2; paragraphs 54-56; external user supplies protection key for rights access (read, write) to protected memory)

Although Beukema does not disclose rendering the memory protection key in the memory command inaccessible by overwriting at least a portion of the memory protection key, such a step to ensure secure deletion of sensitive information in memory is well known in the art. Such a step prevents covert analysis of memory to determine

the value of deallocated memory. For example, Starek discloses it is well known in the art to securely delete sensitive information by overwriting data. (Col. 1:40-53) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to render the memory protection key in the memory command inaccessible by overwriting at least a portion of the memory protection key. One would be motivated to do so to securely remove sensitive information as known to one of ordinary skill. The aforementioned cover the limitations of claims 1, 2, 4, 7-9 and 11-15.

9. Claims 1, 9, 10, 29 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bryant in view of Starek.

10. As per claims 1, 9, 10 and 41, Bryant discloses a memory protection system comprising:

p. a key store storing identifiers of protected memory locations and respective corresponding memory protection keys; and a memory access manager configured to receive a memory command for altering contents of any of the protected memory locations, determine whether the memory command includes a memory protection key corresponding to at least one of said protected memory locations to be altered, if the memory command includes the memory protection key corresponding to each protected memory location to be altered, permit the memory command to proceed, and then render the memory protection key in the memory command inaccessible (fig. 3, reference nos. 485-530; figs. 7

and 9; by virtue of de-allocating memory; see also applicant's specification, pg. 17, lines 19-26);

q. implemented in an electronic device having a memory, the memory comprising the protected memory locations and unprotected memory locations (program requests region of memory to be protected);

r. wherein the memory access manager is further configured to receive memory commands for altering contents of the unprotected memory locations without checking for any memory protection key (only protected memory is verified [see fig. 3]);

s. wherein the memory access manager is configured to further receive a memory read command to read content of a particular protected memory location, the memory access manager to allow the memory read command to proceed to read the content of the particular protected memory location without checking for any memory protection key. (col. 21:3-22)

Although Bryant does not disclose rendering the memory protection key in the memory command inaccessible by overwriting at least a portion of the memory protection key, such a step to ensure secure deletion of sensitive information in memory is well known in the art. Such a step prevents covert analysis of memory to determine the value of deallocated memory. For example, Starek discloses it is well known in the art to securely delete sensitive information by overwriting data. (Col. 1:40-53) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to render the memory protection key in the memory command inaccessible by overwriting

at least a portion of the memory protection key. One would be motivated to do so to securely remove sensitive information as known to one of ordinary skill. The aforementioned cover the limitations of claims 1, 9, 10 and 41.

11. As per claim 29, the rejection of claim 25 under 35 USC 102(b) as being anticipated by Bryant is incorporated herein. Bryant discloses the method further comprising the step of: storing the received data to an unprotected memory location (fig. 1, reference no. 100), wherein rendering the memory protection key in the memory command inaccessible comprises erasing the received data from the unprotected memory location upon completion of the memory command; (by virtue of de-allocating memory; see also applicant's specification, pg. 17, lines 19-26) Although Bryant does not disclose rendering the memory protection key in the memory command inaccessible by overwriting at least a portion of the memory protection key, such a step to ensure secure deletion of sensitive information in memory is well known in the art. Such a step prevents covert analysis of memory to determine the value of deallocated memory. For example, Starek discloses it is well known in the art to securely delete sensitive information by overwriting data. (Col. 1:40-53) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to render the memory protection key in the memory command inaccessible by overwriting at least a portion of the memory protection key. One would be motivated to do so to securely remove sensitive information as known to one of ordinary skill. The aforementioned cover the limitations of claim 29.

12. Claims 16-20, 26-28, 36, 39, 43, 44 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind et al. US 6,976,163 (hereinafter Hind) in view of Bryant.

13. As per claims 16-20 and 43, Hind discloses an electronic device comprising a memory, a wireless receiver configured to receive data relating to a remote software update to be written to the memory, and means to securely update the software files via update rules. (col. 2:38-59; 19:40-46) However, Hind does not disclose ensuring that the update has the proper permission to execute the update in a particular memory region. Bryant discloses an electronic device comprising:

t. a memory; a receiver configured to receive data to be written to the memory; and a memory protection system associating protected memory locations in the memory with respective corresponding keys, and configured to allow the received data to be written to any of the protected memory locations only if the received data includes a key corresponding to the protected memory location to which the received data is to be written and to render the corresponding key in the received data inaccessible after allowing the received data to be written to the protected memory location (fig. 1, fig. 3);

u. wherein the memory comprises unprotected memory locations into which the received data is written (program requests page protection);

v. wherein each key is rendered inaccessible by erasing the received data from the unprotected memory locations where the memory access manager allows the received data to be written to the protected memory locations (by virtue of de-allocating memory; see also applicant's specification, pg. 17, lines 19-26);

w. wherein the memory protection system comprises: a key store storing a mapping table that associates the protected memory locations with the respective corresponding keys; and a memory access manager configured to process a memory command for writing the received data to any of the protected memory locations, determine whether the received data includes the key corresponding to any of the protected memory locations to which the received data is to be written, if the received data includes the key corresponding to a protected memory location to which the received data is to be written, to permit the memory command to proceed, and then render the corresponding key in the received data inaccessible (19:41-20:6);

x. wherein the key store resides at a secure location in the memory outside of the main memory (fig. 1, reference no. 105);

y. wherein the memory protection system is configured to further receive a memory read command to access a particular one of the protected memory locations, perform reading of the particular protected memory location in response to the memory read command, without checking for any memory protection key. (21:3-22)

It would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Hind with the teaching of Bryant. One would be motivated to do so to ensure that the update has the proper permission to execute the update in a particular memory region as disclosed by Bryant. (5:22-30) The aforementioned cover the limitations of claims 16-20 and 43.

14. As per claims 26, 27 and 44, Hind discloses a method to remotely update software via update rules contained in the update; receiving the update comprises receiving, by a wireless receiver. (col. 2:38-59; 19:40-46) However, Hind does not disclose ensuring that the update has the proper permission to execute the update in a particular memory region. Bryant discloses a method of protecting memory in an electronic device, comprising:

z. receiving a memory command to alter a protected memory location; determining whether the received memory command is a memory read command to read the protected memory location, or a memory write command to alter the protected memory location (col. 21:3-21; fig. 3); in response to determining that the received memory command is the memory write command:

iii. identifying a memory protection key corresponding to the protected memory location; determining whether the memory command includes the memory protection key corresponding to the protected memory location; permitting completion of the memory command where the memory command includes the memory protection key corresponding to the

protected memory location (fig. 3, reference nos. 540, 560); and rendering the memory protection key in the memory command inaccessible (by virtue of de-allocating memory; see also applicant's specification, pg. 17, lines 19-26); and

aa. in response to determining that the received memory command is the memory read command, processing the memory read command to read the protected memory location without checking for any memory protection key; (21:15-18)

bb. receiving data to be written to the protected memory location; and generating the memory write command responsive to receiving the data (fig. 1, reference no. 540);

cc. wherein the received data comprises a received key, and wherein generating comprises extracting the received key from the received data and inserting the received key into the memory write command (fig. 3, reference no. 540).

It would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Hind with the teaching of Bryant. One would be motivated to do so to ensure that the update has the proper permission to execute the update in a particular memory region as disclosed by Bryant. (5:22-30) The aforementioned cover the limitations of claims 26, 27 and 44.

15. As per claim 28, the rejection of claim 26 under 35 USC 103(a) as being unpatentable over Hind in view of Bryant is incorporated herein. Neither Hind nor Bryant expressly disclose wherein determining comprises retrieving a modified version of the memory protection key corresponding to the protected memory location, modifying the received key in the memory write command to generate a modified received key, and comparing the modified received key to the modified version of the memory protection key corresponding to the protected memory location; however, it is notoriously well known in the art to use and store a hash value of an identifier as opposed to the original identifier. A hash value uniquely maps an original value to a modified value, such that the modified value is typically much smaller than the original value. Hence, the modified value retains the unique property of the original value but requires less memory and bandwidth requirements to store and communicate the value. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made wherein the determining step comprises retrieving a modified version of the memory protection key corresponding to the protected memory location, modifying the received key in the memory write command to generate a modified received key, and comparing the modified received key to the modified version of the memory protection key corresponding to the protected memory location. One would be motivated to do so to preserve memory and processing resources as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 28.

16. As per claims 36 and 45, Hind discloses a method to remotely update software via update rules contained in the update; wherein the update is received by a wireless receiver. (col. 2:38-59; 19:40-46) However, Hind does not disclose ensuring that the update has the proper permission to execute the update in a particular memory region. Bryant discloses a method of protecting electronic memory, comprising:

dd. configuring a memory store of an electronic device into at least one protected memory location and a key store operable to store an identifier of each protected memory location and a respective corresponding memory protection key; and configuring a processor of the electronic device to provide a memory access manager operable to receive memory commands for altering contents of any of the at least one protected memory location, and for at least one memory command, to determine whether the memory command includes a memory protection key corresponding to at least one protected memory location to be modified, said memory command including the memory protection key corresponding to at least one said protected memory location to be modified, to permit the memory command and then render each corresponding memory protection key in the command inaccessible; (fig. 3, reference nos. 540-570)

ee. wherein configuring the processor further comprises configuring the processor to receive a memory read command to read a particular one of the protected memory locations, and to permit the memory read command to read the particular protected memory location without checking for any memory protection key. (21:3-22)

It would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Hind with the teaching of Bryant. One would be motivated to do so to ensure that the update has the proper permission to execute the update in a particular memory region as disclosed by Bryant. (5:22-30) The aforementioned cover the limitations of claims 36 and 45.

17. As per claim 39, Bryant further suggests a computer-readable medium storing instructions for performing the method of claim 36. (fig. 1)

18. Claim 42 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hind in view of Bryant and Starek.

19. As per claim 42, the rejection of claim 16 under 35 USC 103(a) as being unpatentable over Hind in view of Bryant is incorporated herein. In addition, Hind in view of Bryant suggest a volatile storage having unprotected memory locations, the memory protection system configured to download the received data including the key to the unprotected memory locations of the volatile storage prior to writing the received data to the protected memory locations (Hind, fig. 5, reference no. 402; Bryant, fig. 1, reference no. 100), and the memory protection system to render the key inaccessible. (by virtue of de-allocating memory; see also applicant's specification, pg. 17, lines 19-26) Although Bryant does not disclose rendering the memory protection key in the memory command inaccessible by overwriting at least a portion of the memory

protection key, such a step to ensure secure deletion of sensitive information in memory is well known in the art. Such a step prevents covert analysis of memory to determine the value of deallocated memory. For example, Starek discloses it is well known in the art to securely delete sensitive information by overwriting data. (Col. 1:40-53) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to render the memory protection key in the memory command inaccessible by overwriting at least a portion of the memory protection key. One would be motivated to do so to securely remove sensitive information as known to one of ordinary skill. The aforementioned cover the limitations of claim 42.

20. Claims 1 and 3-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over England et al. USPN 7,194,092 (hereinafter England) in view of Starek.

21. As per claims 1 and 3-6, England discloses a memory protection system comprising:

ff. a key store storing identifiers of protected memory locations and respective corresponding memory protection keys; and a memory access manager configured to receive a memory command for altering contents of any of the protected memory locations, determine whether the memory command includes a memory protection key corresponding to at least one of said protected memory locations to be altered, if the memory command includes the memory protection key corresponding to each protected memory location to be altered,

permit the memory command to proceed, and then render the memory protection key in the memory command inaccessible (col. 10:41-51; by virtue of de-allocating memory; see also applicant's specification, pg. 17, lines 19-26);

gg. wherein the identifiers comprise names of protected files in a memory; wherein the identifiers identify data entries in a protected memory; (10:31-35; 16:33-37)

hh. wherein each of the memory protection keys comprises a modified version of a data sequence; wherein the modified version comprises a hash of the data sequence. (10:41-51; 17:1-30; 17:57-18:14)

22. Although England does not disclose rendering the memory protection key in the memory command inaccessible by overwriting at least a portion of the memory protection key, such a step to ensure secure deletion of sensitive information in memory is well known in the art. Such a step prevents covert analysis of memory to determine the value of deallocated memory. For example, Starek discloses it is well known in the art to securely delete sensitive information by overwriting data. (Col. 1:40-53) Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to render the memory protection key in the memory command inaccessible by overwriting at least a portion of the memory protection key. One would be motivated to do so to securely remove sensitive information as known to one of ordinary skill. The aforementioned cover the limitations of claims 1 and 3-6.

Conclusion

23. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JUNG KIM whose telephone number is (571)272-3804. The examiner can normally be reached on FLEX.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Jung Kim/
Primary Examiner AU 2132